Cassandra Crossing/ L’impercettibile robustezza del software non aggiornato

(589) —La “Frenesia dell’aggiornamento” sfida il “Se funziona, non lo toccare”. Cosa possiamo dire nel caso MS/Crowdstrike”?

Cassandra Crossing/ L’impercettibile robustezza del software non aggiornato
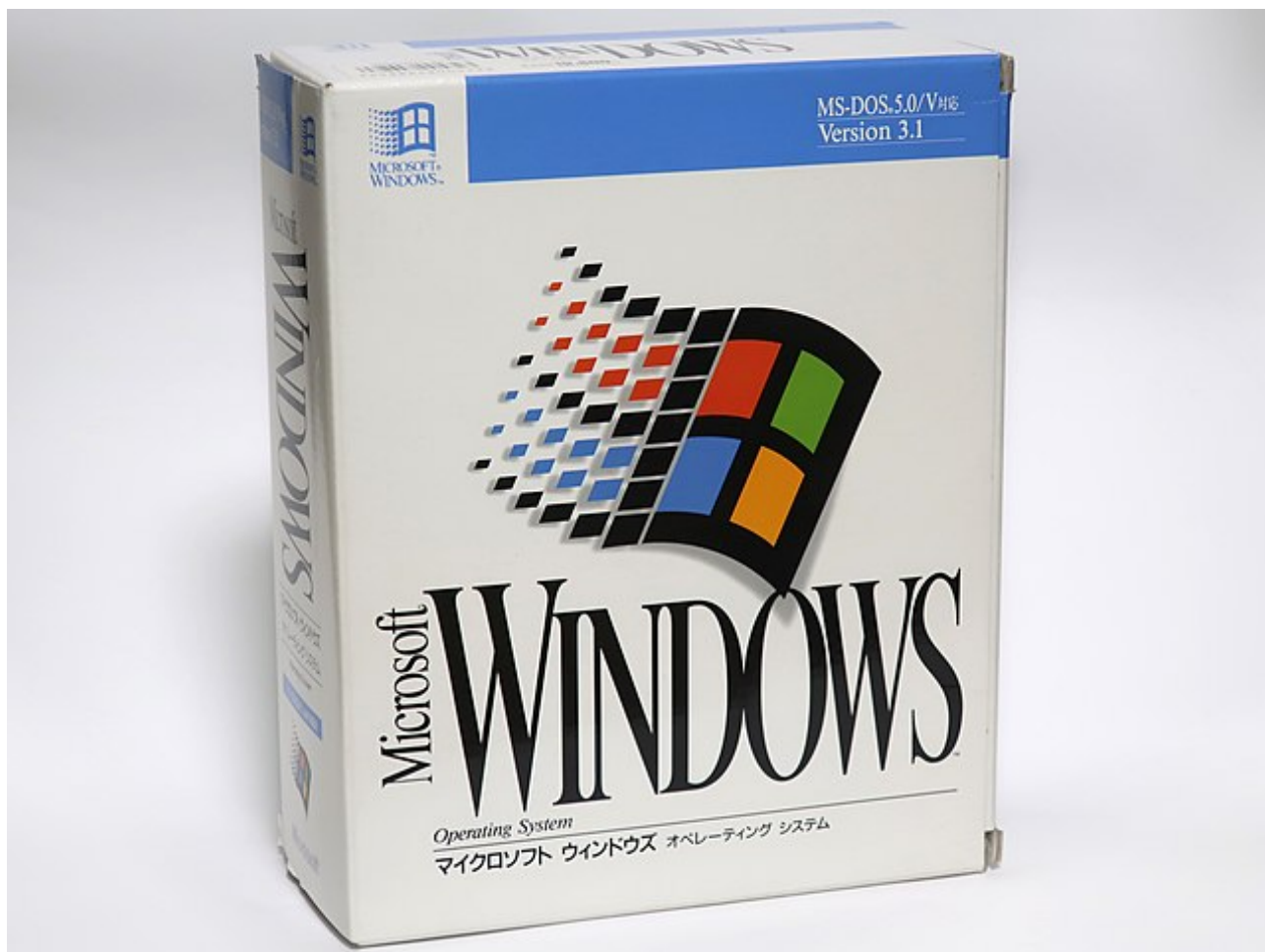
Figure 1: By Darklanlan—Own work, CC0, https://commons.wikimedia.org/w/index.php?curid=95530546

(589) —La “Frenesia dell’aggiornamento” sfida il “Se funziona, non lo toccare”. Cosa possiamo dire nel caso MS/Crowdstrike”?

22 luglio 2024—Ai tempi dell’università, quando Cassandra gestiva in grande economia una decrepita 850 Sprint, il suo compianto meccanico di fiducia, a cui prima di un viaggio fu chiesto di “*dare un’occhiata*” all’auto, si rifiutò di aprire il cofano della macchina, perché non c’era nulla che non andasse. All’epoca sembrò una fissazione del simpatico vecchietto, e questo perché allora Cassandra era (oggi un po’ meno) un’ingenua ed un po’ saputella giovinetta, convinta che buone intenzioni e buone azioni si traducessero sempre nei risultati attesi, ovviamente positivi.

Beata gioventù, molto ti si può scusare, però …

Agli addetti ai lavori, invece, nulla si può scusare; sono pagati per fare le scelte giuste, e se non le fanno, o ne fanno di sbagliate, è giusto che ricevano (almeno) le meritate critiche.

Chiunque abbia dedicato un minimo di attenzione, anche solo di sfuggita, all'*affaire* Microsoft/Crowdstrike, avrà capito perfettamente che si è trattato di un problema derivante da una fiducia cieca ed assoluta nei prodotti software di un'azienda di ottima reputazione, e soprattutto dei relativi aggiornamenti.

Questa fiducia, affiancata a lodevoli e pressanti richieste delle normative di mantenere sempre aggiornato il software, ha fatto si che l'aggiornamento automatico fosse lasciato acriticamente abilitato.

Si tratta spesso di un'ottima idea, tant'è che tutte le applicazioni ed i sistemi operativi lo fanno ormai come default, e gli utenti si guardano bene dal disabilitarlo.

Ma è pur vero che l'applicazione di una soluzione software ad un intero sistema informativo, **senza una buona dose di pensiero competente**, è ciò di cui è lastricata la strada, molto, molto in discesa, che conduce al cyber-inferno.

Non è qui rilevante che il software di Crowdstrike sia in grado di fare bene il suo lavoro, e che sia una componente utile per mantenere la sicurezza di un sistema informativo. L'applicazione a tappeto di un aggiornamento su sistemi critici è una cosa azzardata, soprattutto perché l'attività di testing sugli aggiornamenti prima di rilasciarli è in conflitto con la comprensibile urgenza di diffonderli.

Crowdstrike non era nemmeno nuova a questo tipologia di problemi; si veda ad esempio questo thread di Reddit;

E' invece l'aggiornamento contemporaneo e forzato di un software fornito a scatola chiusa, pur considerato come elemento di sicurezza di un sistema informativo, ad essere una pessima idea, un rischio evidente da considerare con attenzione. Nessuno se lo può permettere, se il sistema deve fare "qualcosa di importante". Si fanno invece test esaustivi, poi aggiornamenti su un piccolo gruppo di utenti selezionati, e solo se tutto va bene si procede all'aggiornamento globale (che in questo caso vuol dire "planetario", magari a scaglioni.

Altrimenti, quando applicata in sistemi informativi molto complessi e carenti di gestione e manutenzione, anche una idea virtuosa diventa alla fine un incredibile autogol. Mai come nell'informatica vale infatti il detto "*Il Diavolo sta nei dettagli*".

Lo dimostra, per lo stesso motivo ma con modalità completamente diverse, la vicenda Solarwinds; anche in quel caso proprio l'applicazione acritica ed automatica degli aggiornamenti è stata la porta della più grande violazione di sicurezza informatica che la storia (fino ad oggi) ricordi.

Ma procediamo con ordine, Cassandra leggeva oggi una notiziola, largamente ripresa e commentata dalla stampa, che la compagnia aerea Southwest aveva comunicato di non aver avuto nessun danno durante la tempesta Microsoft/Crowdstrike "*perché una larga parte dei suoi sistemi usava ancora Windows 3.1*" (altro ricordo di gioventù, è uscito 32 anni fa) .
Il fatto e la spiegazione sono assolutamente veri e corretti, anche se la situazione è un po' più variegata di così, come questo articolo di Forbes ben descrive (giornalisti italiani, prendete esempio!)

Southwest è stata per questo *presa per i fondelli* dai media di tutto il mondo (anche se invece invidiata dai CISO e CTO di molte grandi compagnie aeree). E questo è contemporaneamente ingiusto ed errato.

E' pur vero che la compagnia era precedentemente finita su Wikipedia come "*caso esemplare*" per una serie di malfunzionamenti, perlopiù organizzativi, avvenuti durante il periodo natalizio del 2022, che avevano avuto un impatto devastante sull'azienda e sui suoi viaggiatori.

Ma non è il caso di oggi. Southwest questa volta ha tratto profitto dalla sua arretratezza, e dobbiamo capire il perché. Veniamo quindi al punto, come certo anelano anche i 24 indefettibili lettori.

In un sistema software che sia passabilmente ben gestito dal punto di vista della sicurezza, cosa è preferibile? Che vi girino vecchie macchine (magari virtuali) con Windows 3.1/95/XP, oppure che vengano installati a tappeto pezzi di software non verificati provenienti dall'esterno?

La risposta dovrebbe essere evidente. Un software non aggiornato non è pericoloso "di per sé", deve semplicemente essere impiegato, come tutti gli altri software, in maniera affidabile e sicura.

Al contrario, dare una una fiducia assoluta ad un fornitore, sull'altare della frenesia degli aggiornamenti, è dimostratamente errato.

Affidabilità; se un software gira da 30 anni e fa il suo lavoro, la sua vetustà non è un motivo per dismetterlo, anzi … ricordatevi del mio meccanico. Il sistema informativo che lo contiene deve semplicemente essere gestito adeguatamente per quanto riguarda la sicurezza.

Sicurezza; un software vecchio di 30 anni ha certamente più falle note di quelli recenti. Ma se opportunamente isolato ed amministrato, secondo un opportuna "postura di sicurezza" dell'azienda, è un software come un altro, da impiegarsi o meno sulla base di una valutazione corretta di molte esigenze, anche contrastanti tra loro. Ma non è una cosa "*sbagliata*" di per sé. E sì, questo è vero anche se si tratta di un vecchio sistema operativo, notoriamente fallato, come Windows 3.1.

Infatti, visto che le risorse economiche dedicate ai sistemi informativi sono sempre limitate (per usare un eufemismo), il nuovo non "paga" necessariamente, perché è impossibile avere sviluppi software ben fatti ed accuratamente testati; alla fine, inevitabilmente, succede che la prima versione del software che non schianta subito diventa quella definitiva, va in produzione e li resta per sempre, in attesa di diventare il prossimo "*vecchio software*".

Meglio allora un già vecchio software che, se non è stato mai attaccato ed ha funzionato per tanto tempo, in quel ruolo è evidentemente abbastanza adeguato.

Quindi Southwest, che pare avesse addirittura sulle scrivanie di alcuni dipendenti macchine Windows 3.1, aveva ragione?

Difficile dirlo, ed in questa sede non ci interessa più di tanto. Se fosse vero, probabilmente non erano connesse ad Internet ed i dipendenti non ci leggevano la posta, perché altrimenti sarebbero durate meno di 30 minuti e poi sarebbero cadute preda di una botnet, oppure sarebbero state vittima di malware al primo click incauto di un dipendente.

Resta comunque dimostrato, proprio perché erano certamente vulnerabili, che se le macchine Windows 3.1 di Southwest hanno funzionato normalmente per anni, erano in qualche modo gestite "*bene*" od almeno in maniera "*sufficiente*" dal punto di vista della sicurezza, ed anche ovviamente dell'affidabilità.

Hanno superato una "*tempesta informatica perfetta*" a cui i sistemi moderni non hanno retto, e questo deve far pensare, non suscitare risa.

Quando le risorse economiche per gestire un sistema informativo sono limitate ed insufficienti, cioè sempre, i teorici della gestione dei sistemi informativi devono essere affiancati da sistemisti

di esperienza (qualcuno ha detto “vecchi”?) che lavorino in loco e conoscano la storia dei sistemi su cui lavorano, e le loro voci devono essere ascoltate con pari o superiore dignità.

Ricordate che gli aerei, come previsto a suo tempo da Cassandra, hanno già cominciato a cadere dal cielo per problemi software, facendo centinaia di morti.

Le prossime ondate di disastri informatici globali arriveranno, inevitabili come le maree, e prima o poi, probabilmente più prima che poi, capiterà che per un aggiornamento frettoloso, invece dei miliardi di dollari, dovremo contare i morti. E potrebbero essere molti di più.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica “Quattro chiacchiere con Cassandra”
Lo Slog (Static Blog) di Cassandra
L’archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on July 23, 2024.

Canonical link

Exported from Medium on August 27, 2025.